RSAC 2025 Conference

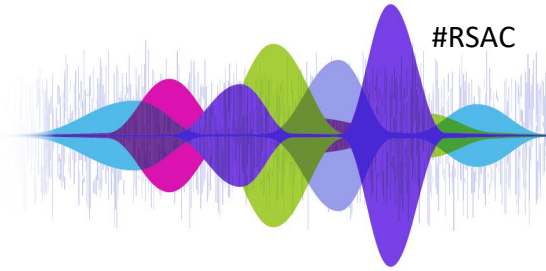
Many Voices.
One Community.

SESSION ID: ANI-T02

Is It Getting Worse Out There?
An Honest Analysis of Cyber Risk Trends

Dr. Wade Baker

Partner, Cyentia Institute
Professor, Virginia Tech
https://www.linkedin.com/in/drwadebaker/



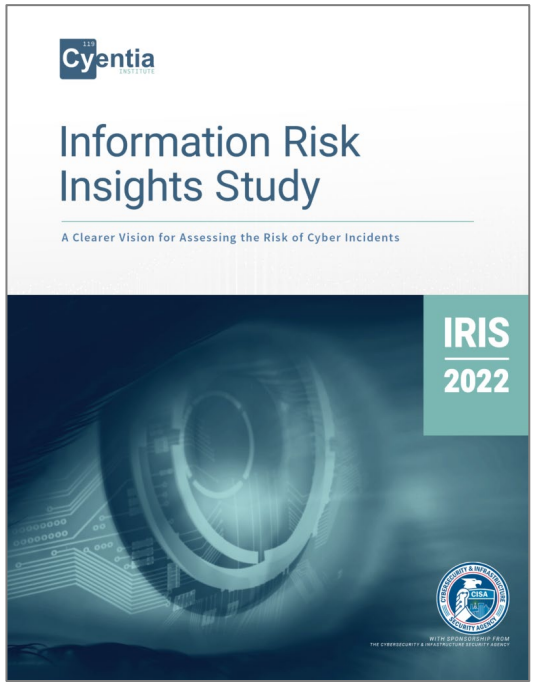
Disclaimer

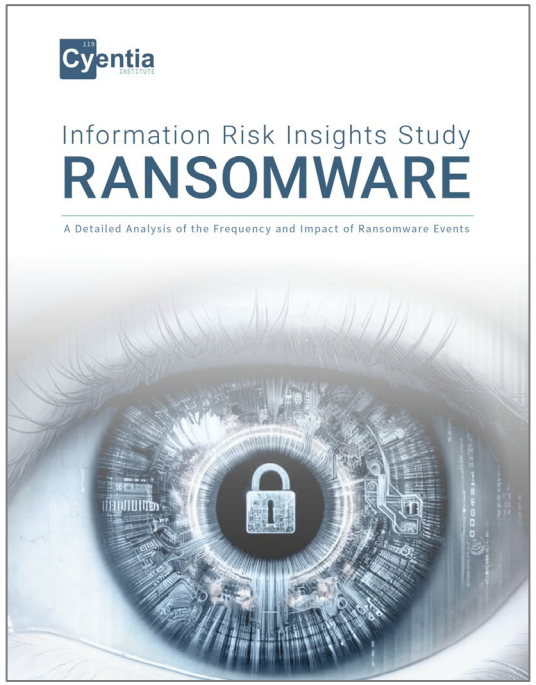
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

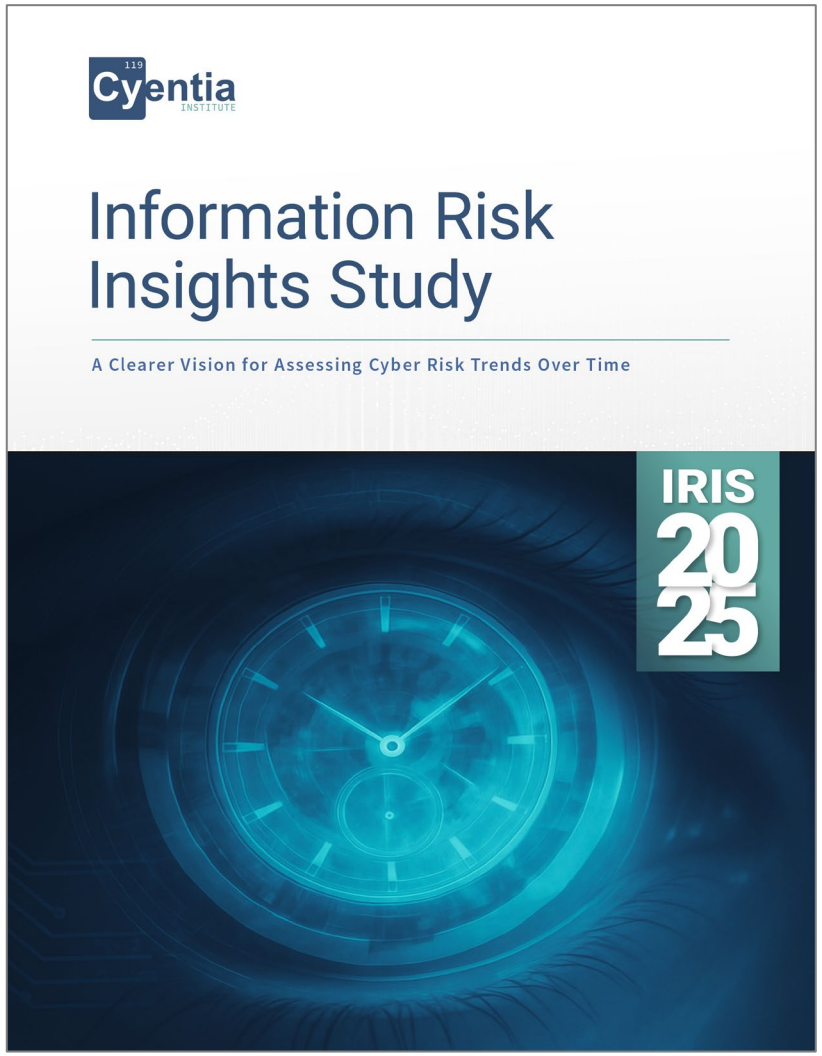
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

CISA-sponsored cyber risk research by Cyentia




Cyentia
Information Risk Insights Study
RANSOMWARE
A Detailed Analysis of the Frequency and Impact of Ransomware Events



Free download: www.cyentia.com/iris

Data & Methodology

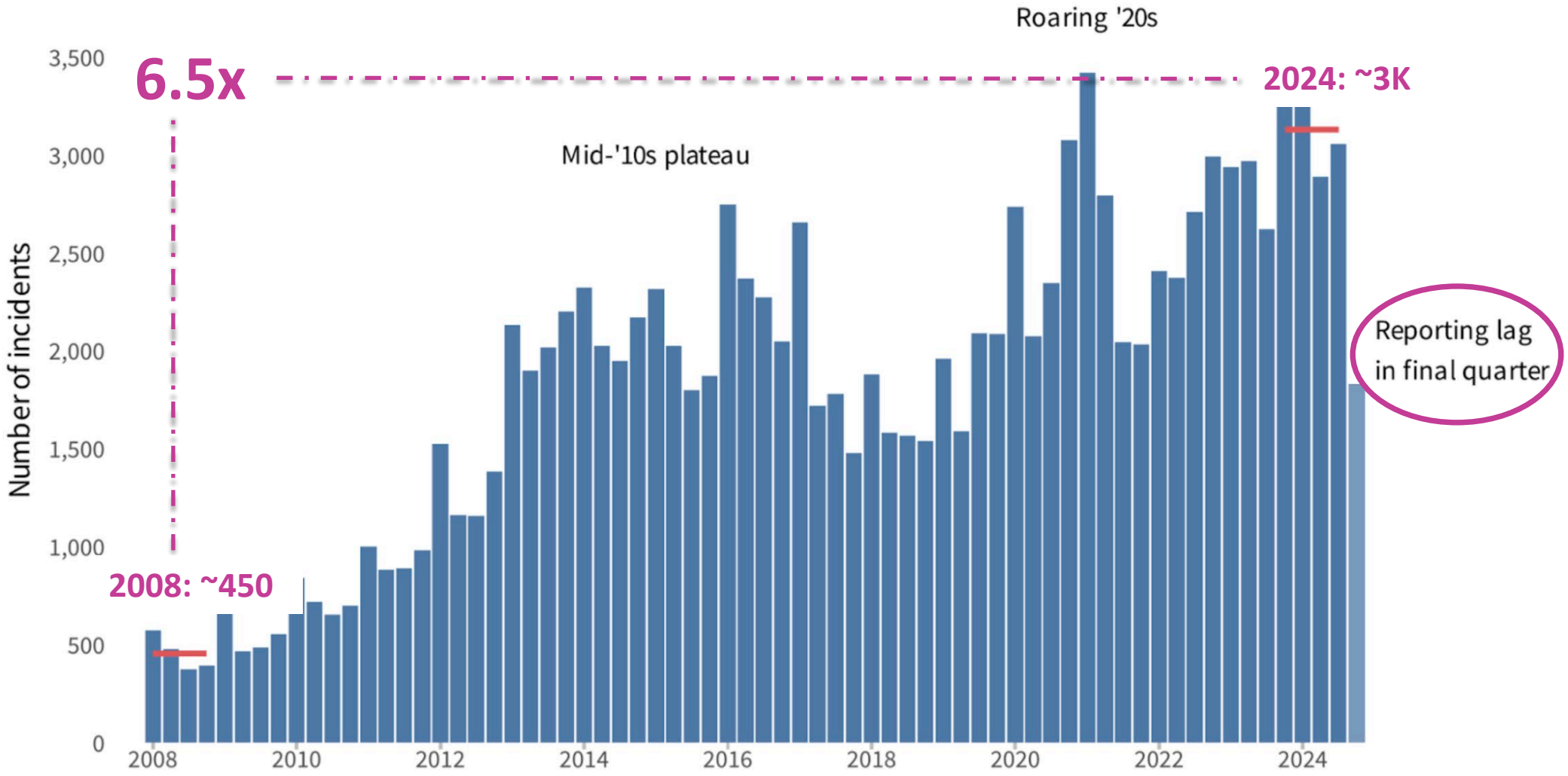
- Base dataset: Zywave (formerly Advisen) Cyber Loss Data
  - Widely used in insurance and reinsurance industry for risk models
  - Contains over 125,000 confirmed security incidents spanning 20+ years
  - Compiled from public info, such as breach disclosures, company filings, litigation details, and Freedom of Information Act requests
  - Most comprehensive source of cybersecurity incidents and losses
- Cyentia does extensive processing of this base dataset to extend and enrich it for cyber risk analysis

RSAC 2025 Conference

Are security incidents becoming more common?

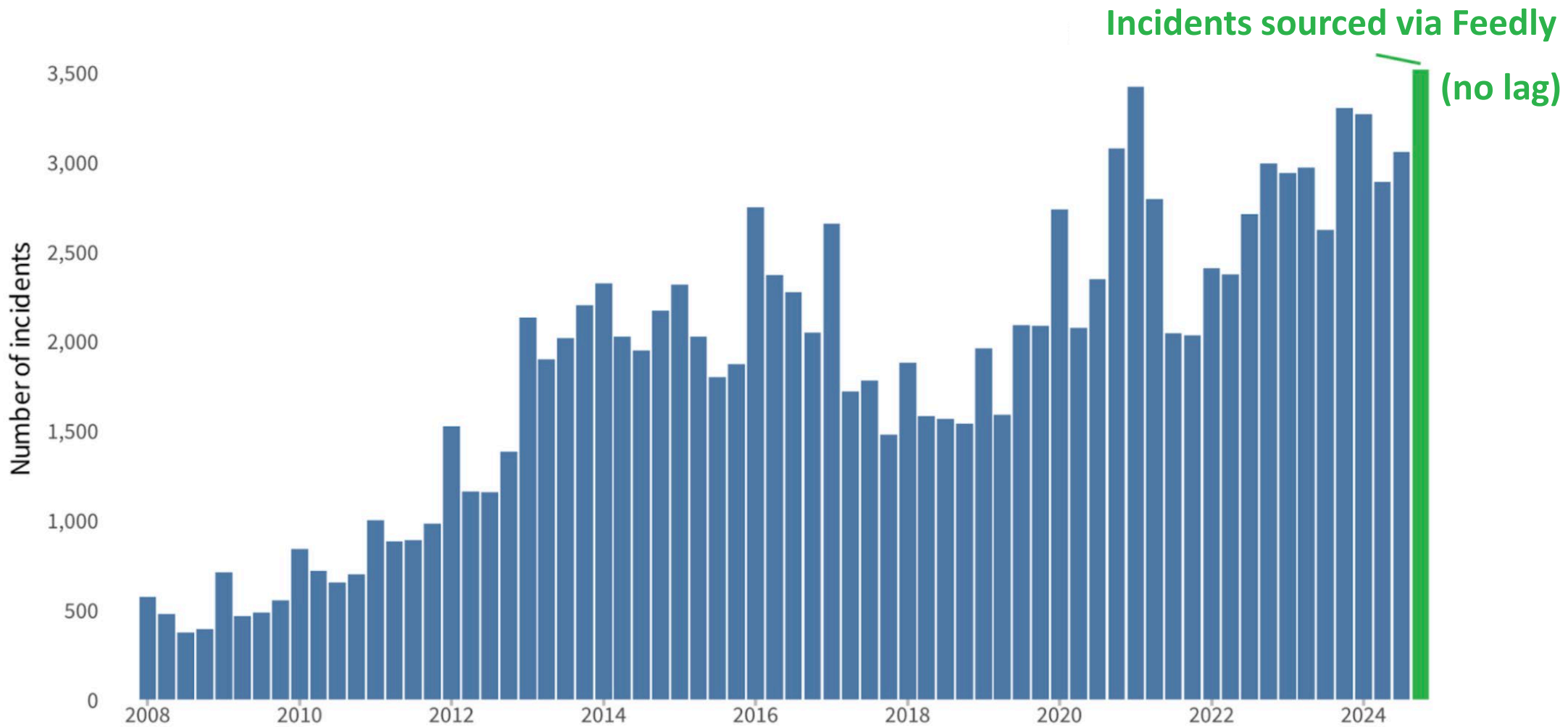
Many Voices.
One Community.

650% more incidents reported each quarter



Number of security incidents publicly reported or discovered each quarter

650% more incidents reported each quarter

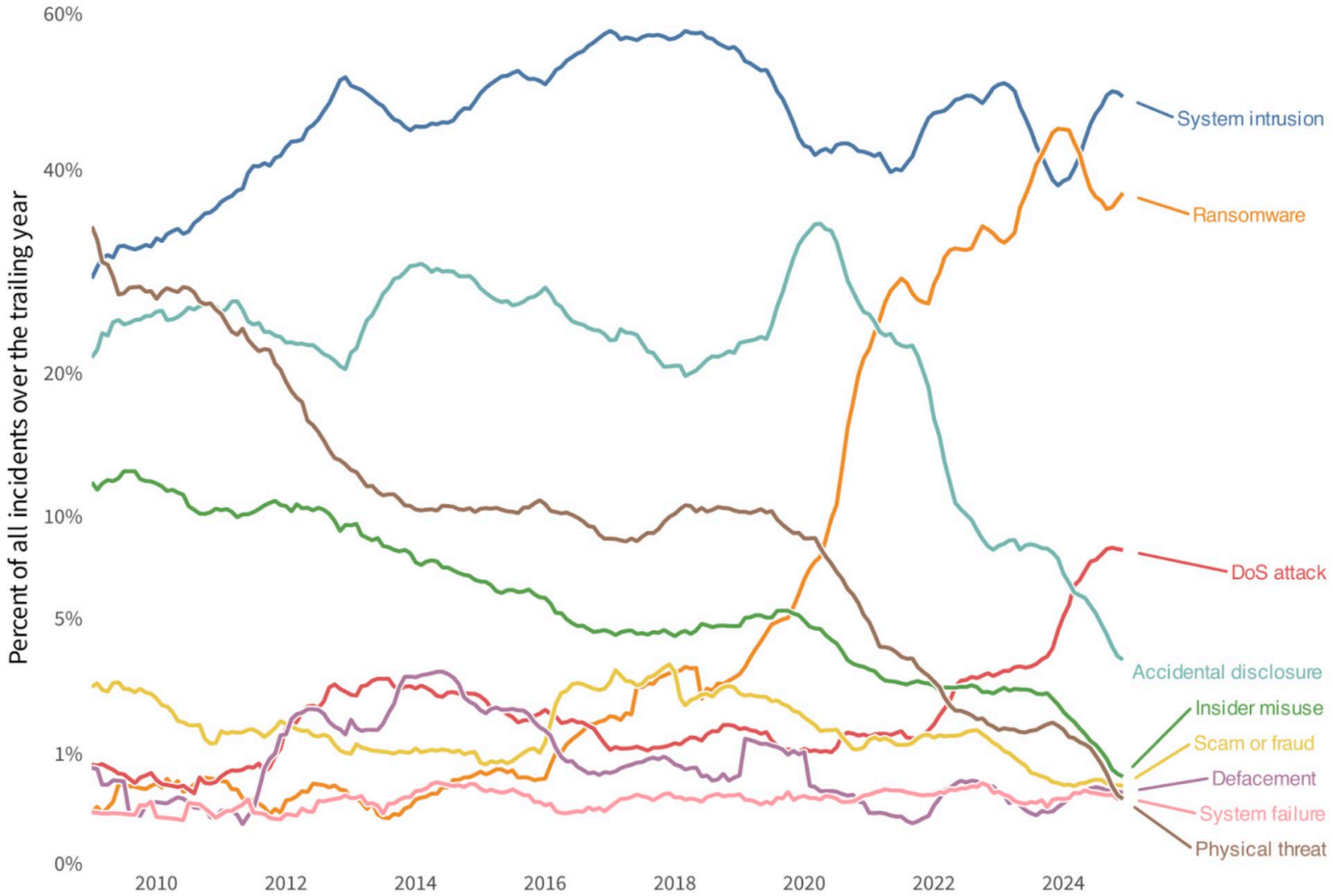


Number of security incidents publicly reported or discovered each quarter

Cyentia INSTITUTE

RSAC 2025 Conference

Trends vary among different types of incidents



Relative frequency of incident patterns over time (rolling 12 months)

Increasing:
Ransomware, DDos

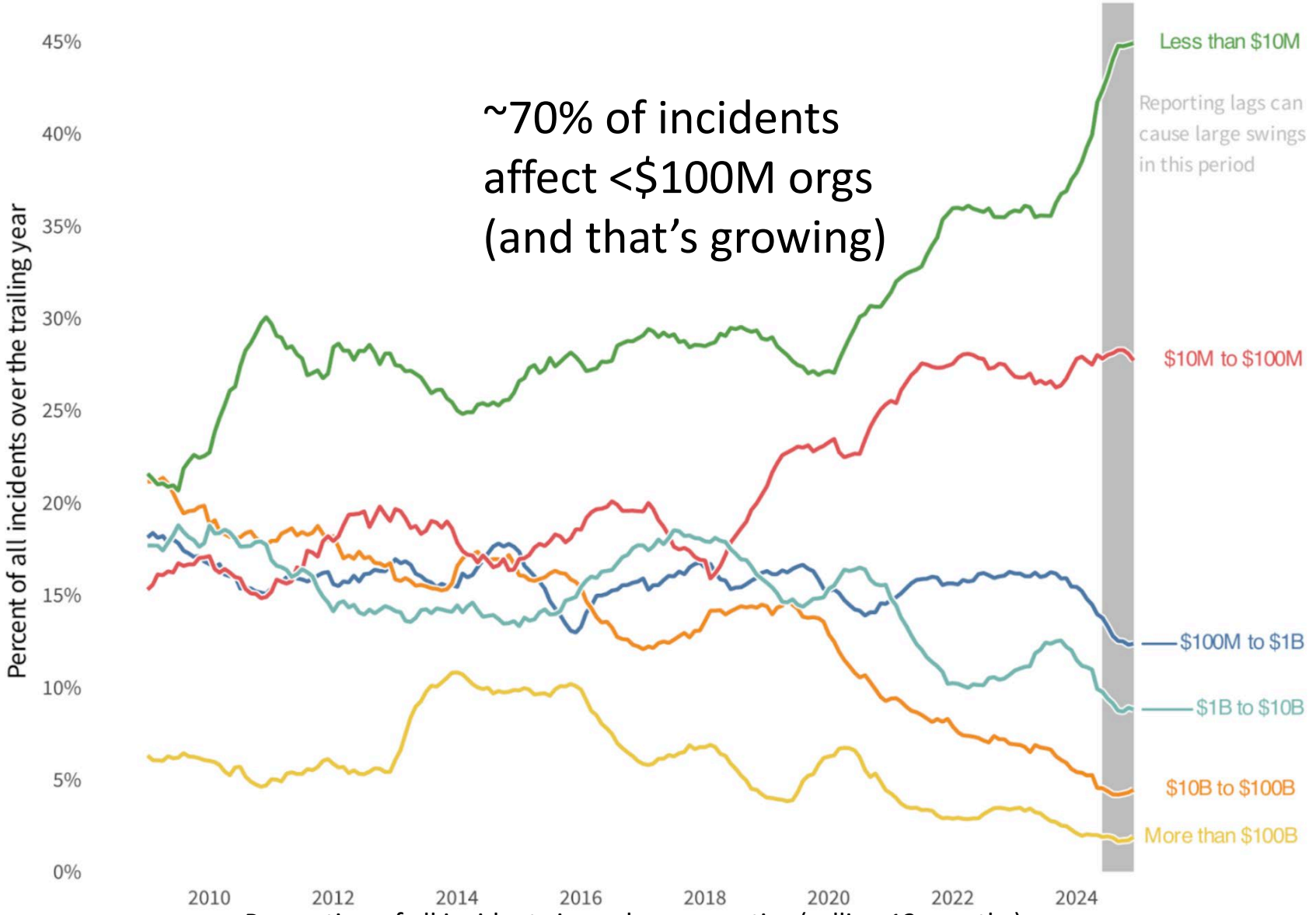
Decreasing:
Accidental disclosure,
insider misuse,
Physical threats
Defacement

RSAC™ 2025 Conference

Do incident trends differ across organizations?

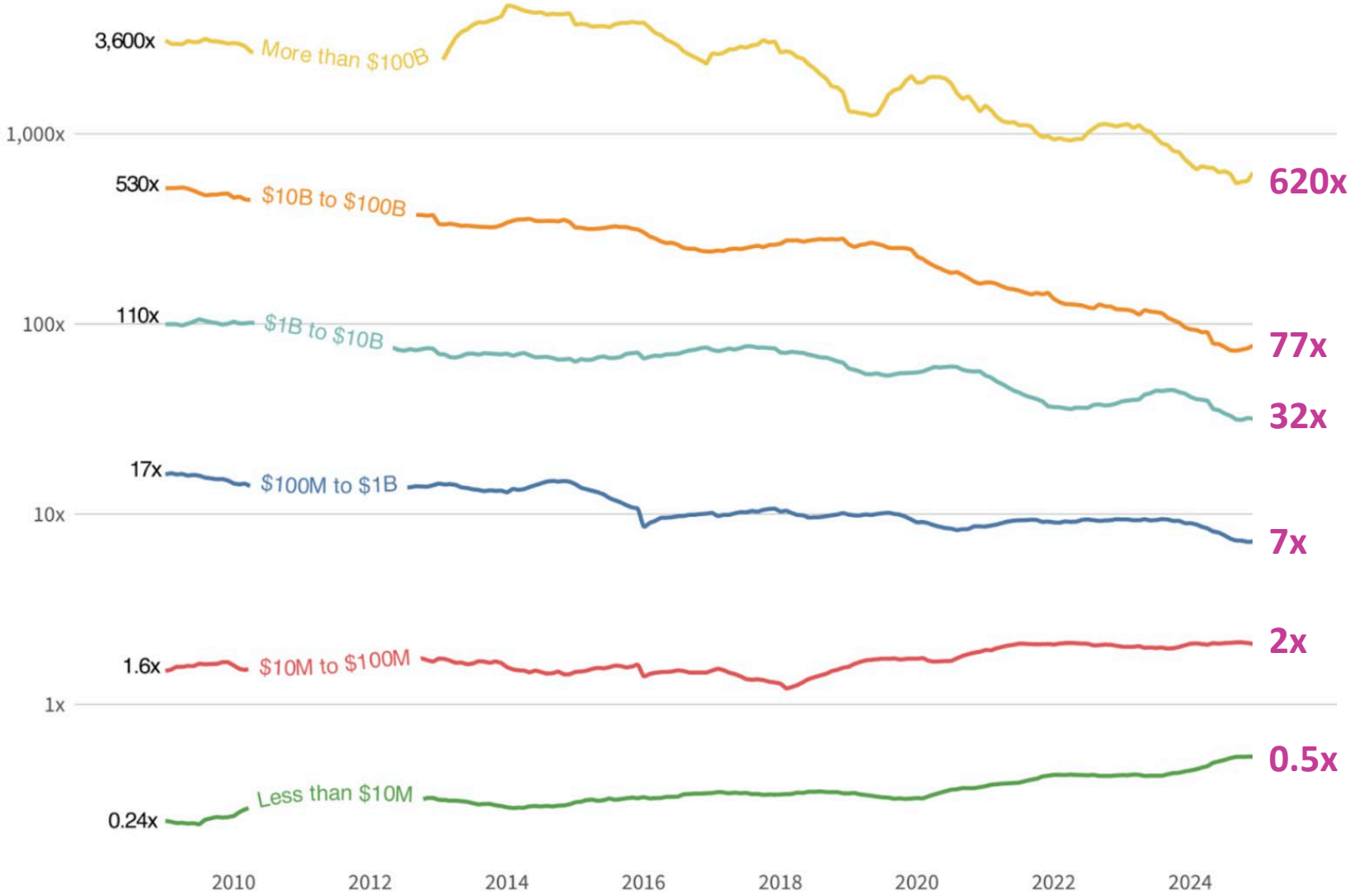
Many Voices.
One Community.

Overall, more incidents affect smaller firms…



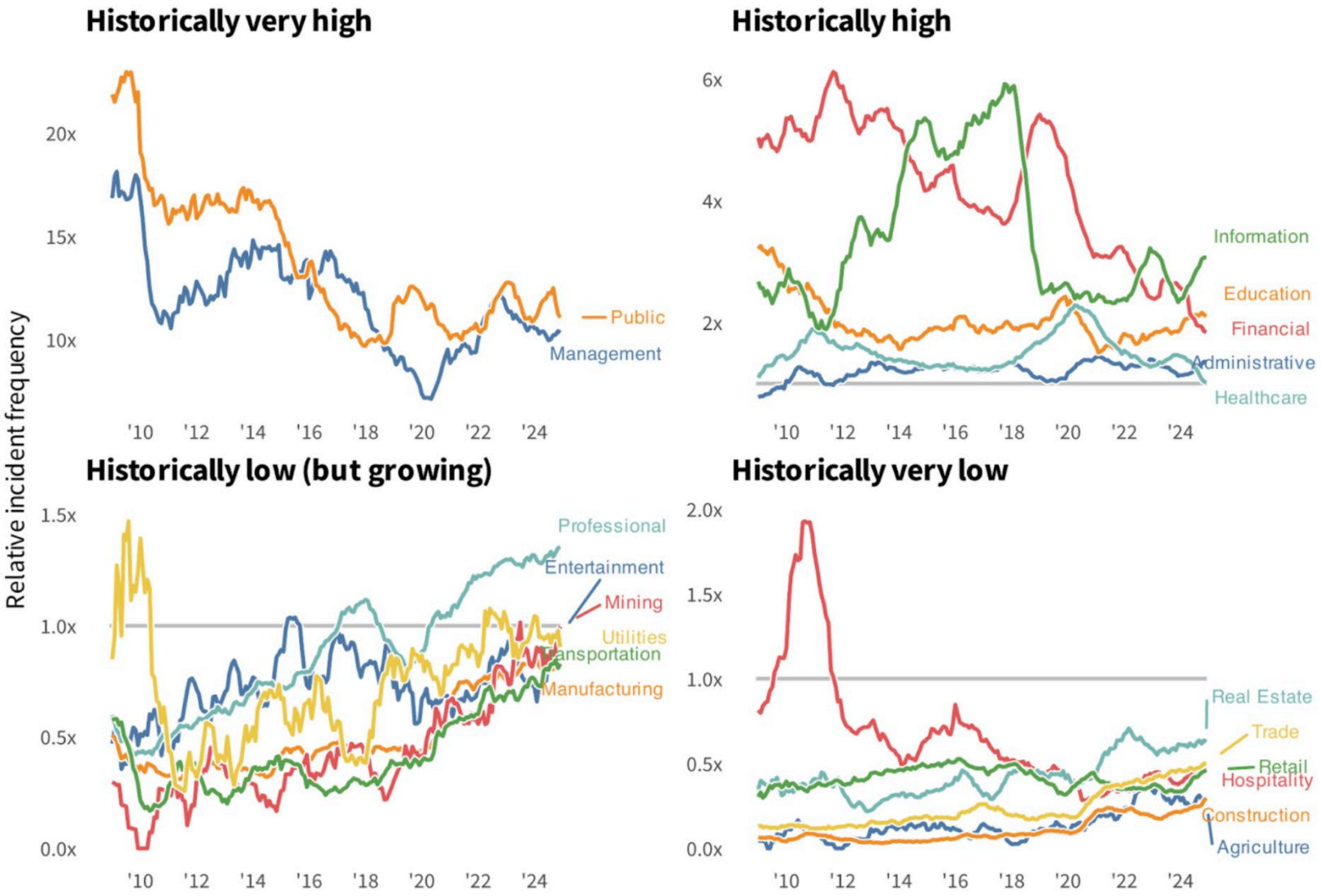
Proportion of all incidents in each revenue tier (rolling 12 months)

…but relative frequency higher for large orgs



Relative number of incidents to number of firms in each revenue tier

Sectors differ historically for relative frequency



Relative incident frequency normalized by number of firms in each sector

Cyentia INSTITUTE

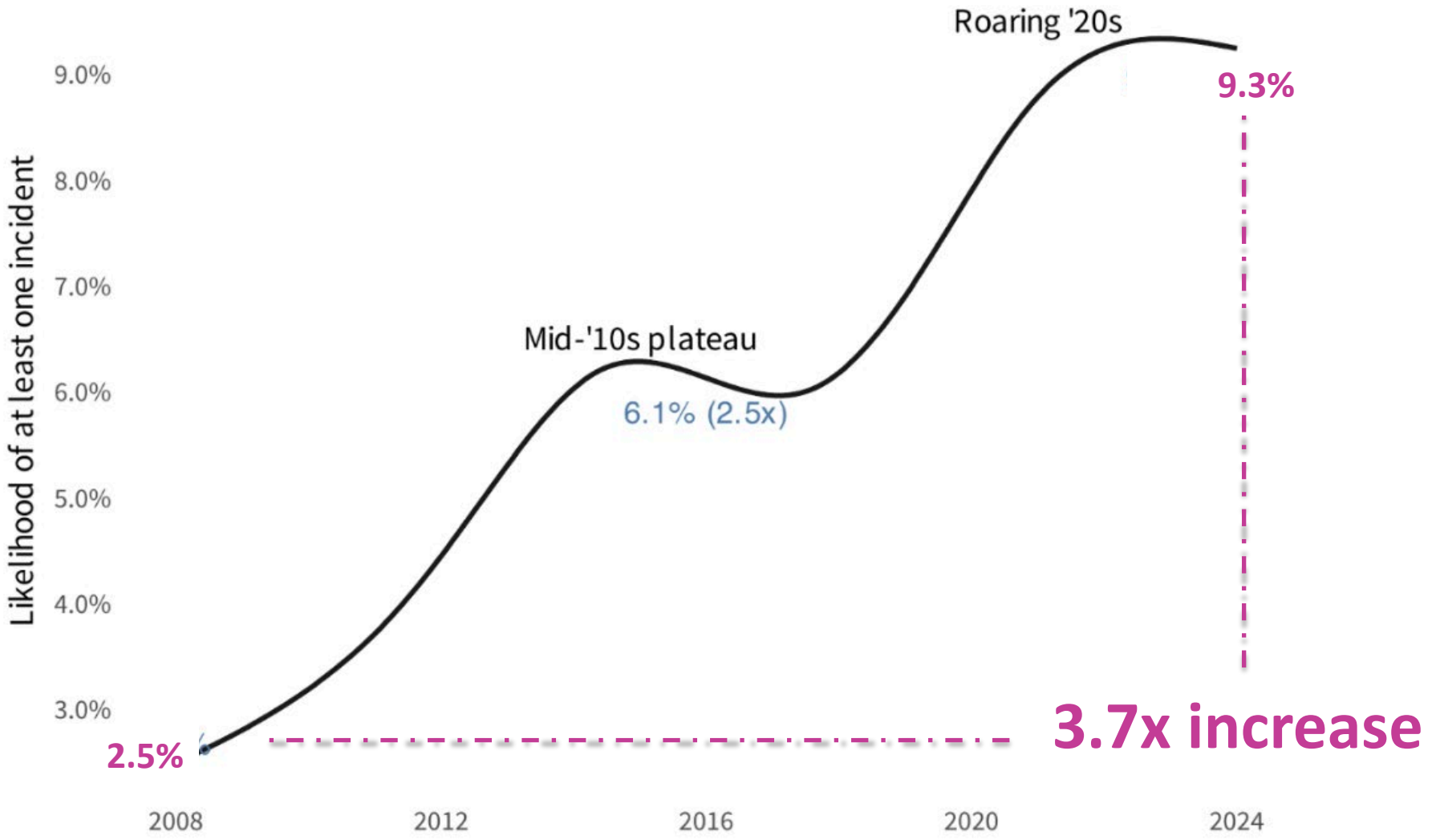
RSAC 2025 Conference

RSAC™ 2025 Conference

Is the probability of incidents increasing?

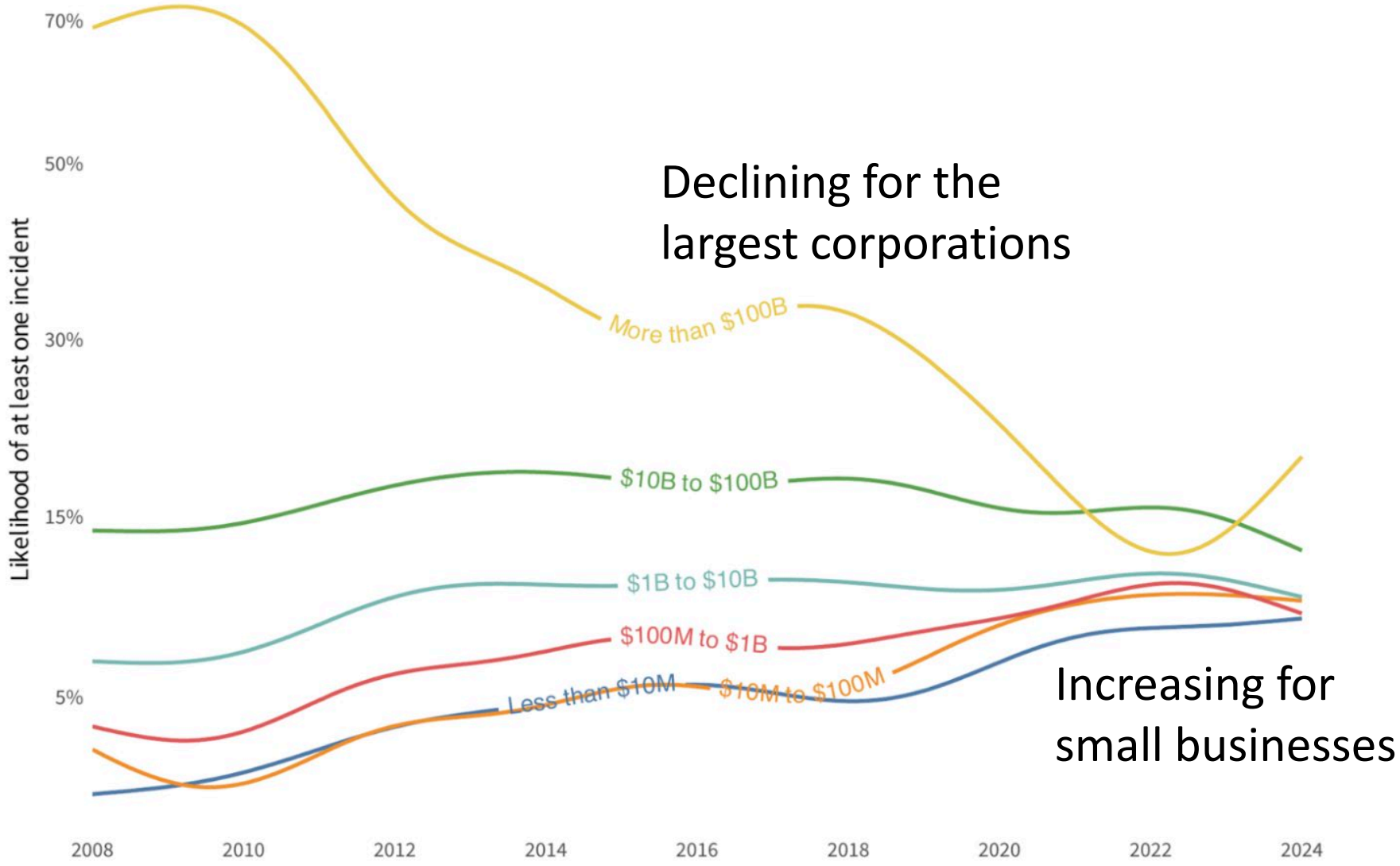
Many Voices.
One Community.

Overall, firms 3.7x more likely to have incidents…



Historical probability of a firm having an incident in the next year

…but that trend varies for large vs. small firms…



Declining for the largest corporations

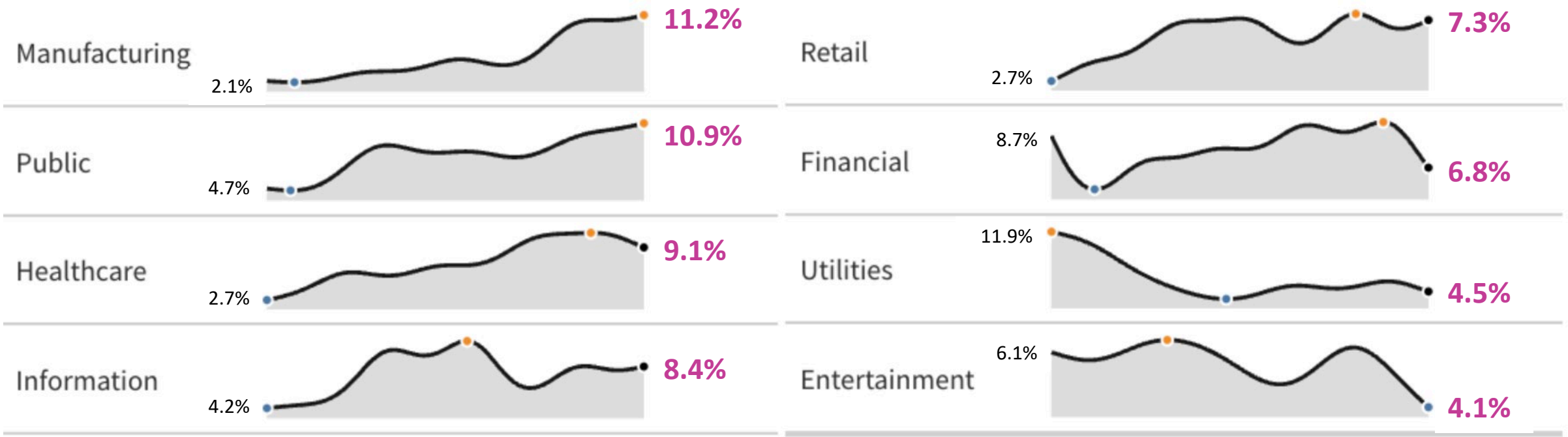
Increasing for small businesses

Annualized incident probability for firms in each revenue tier

Cyentia INSTITUTE

RSAC 2025 Conference

…and differs widely among industries as well



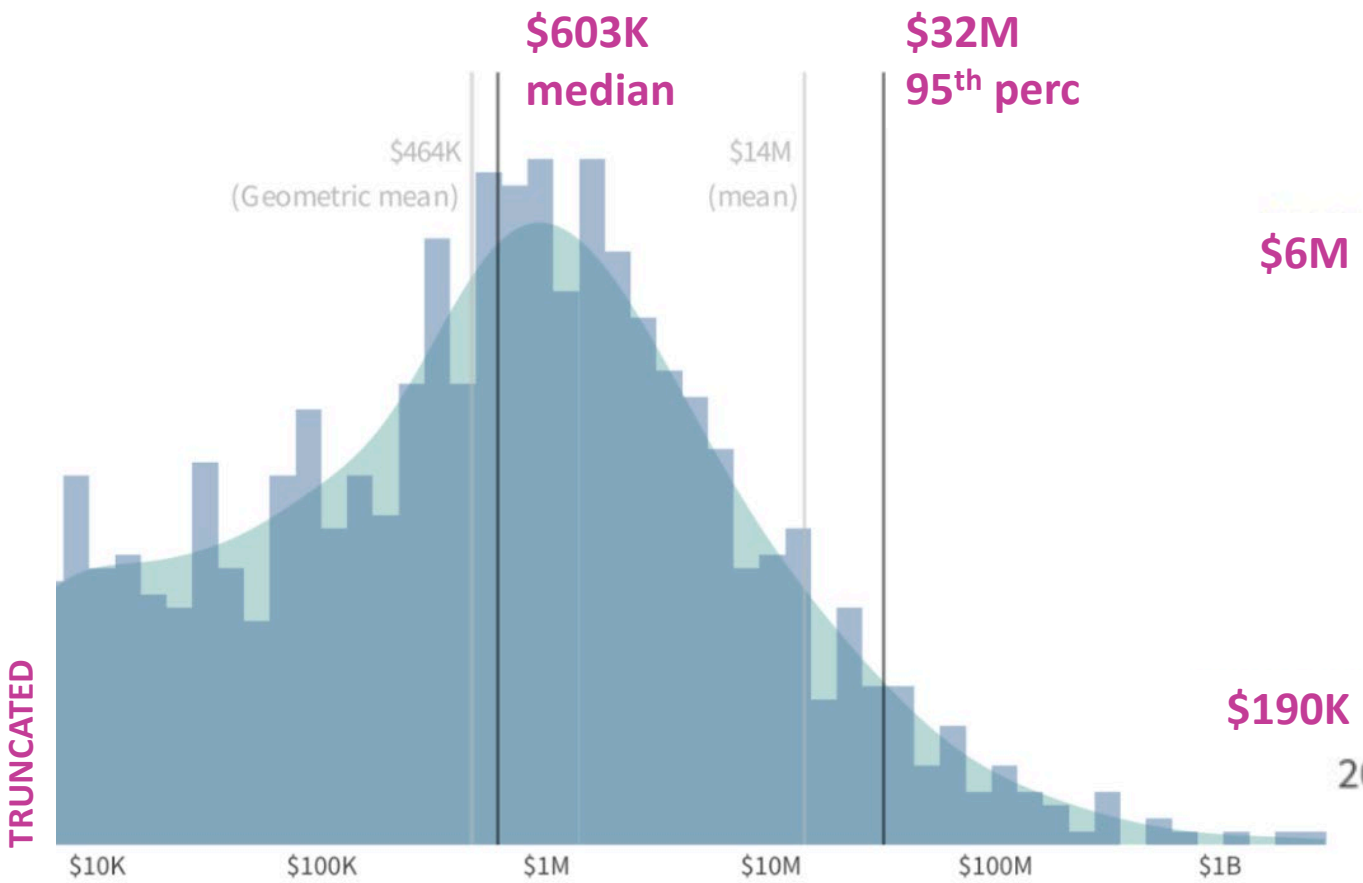
Annualized incident probability for firms in each sector

RSAC™ 2025 Conference

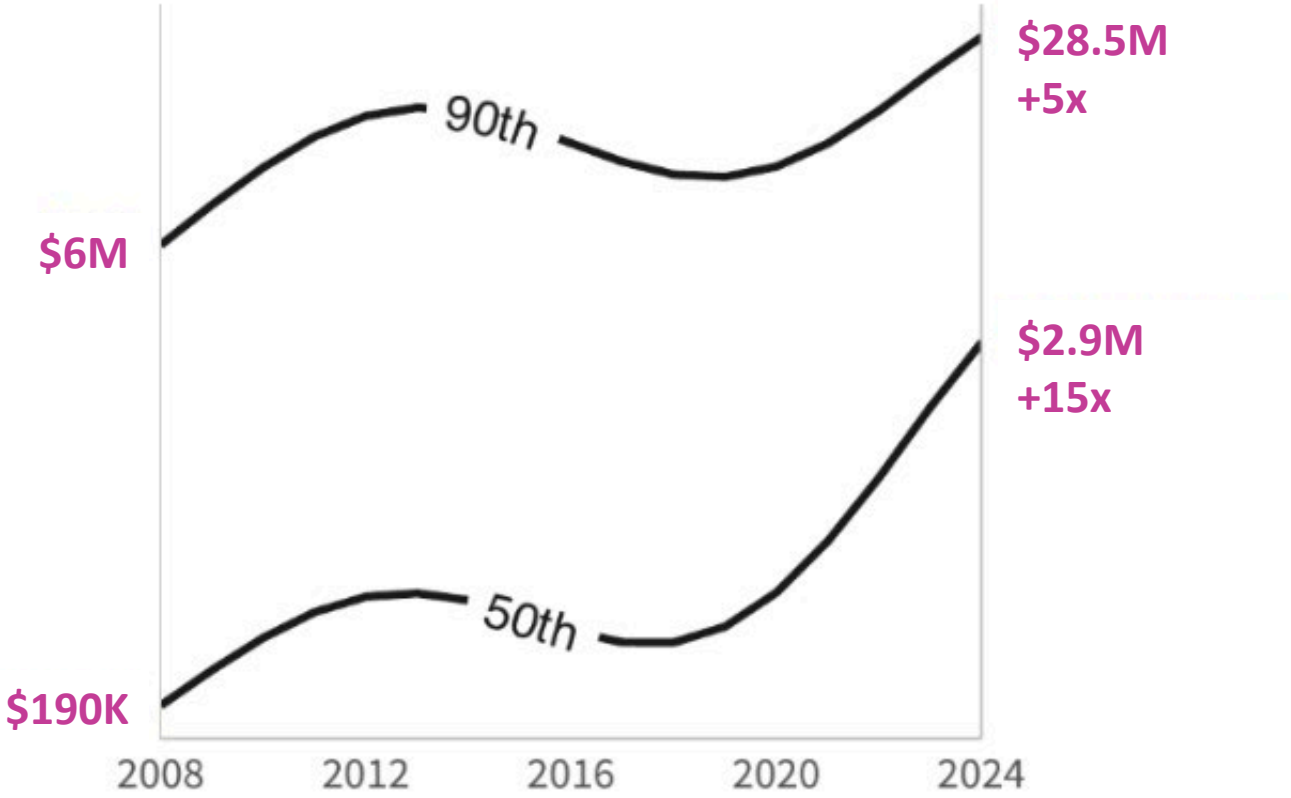
Have security incidents gotten more costly?

Many Voices.
One Community.

Median losses 15 times higher; extreme up 5X



Distribution of reported losses for security incidents from 2015 to 2024

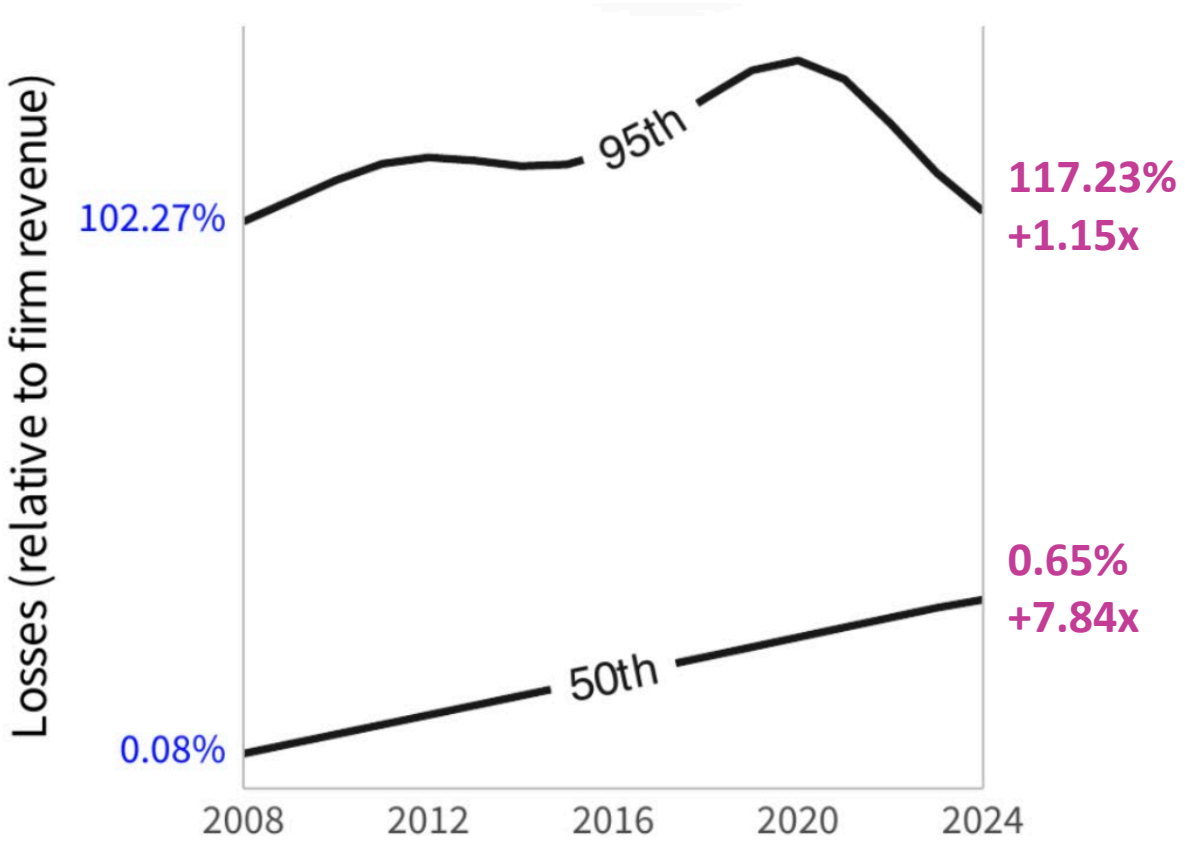


Trend analysis of median and 90th percentile event losses.

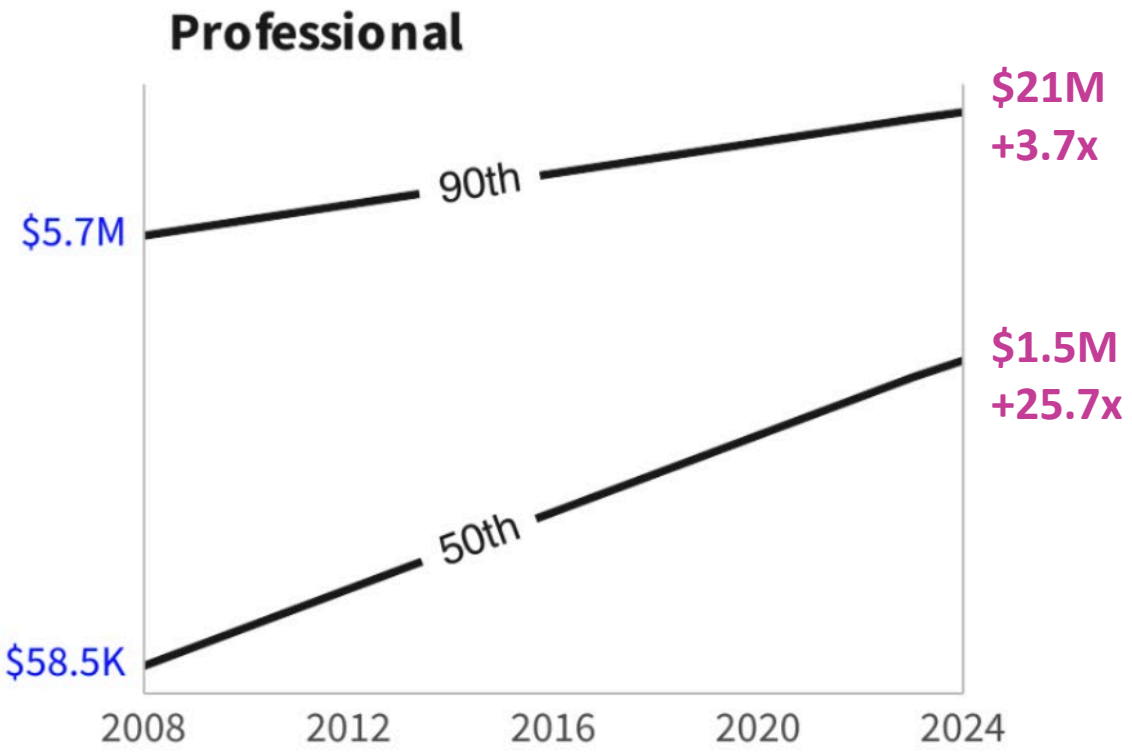
Costs growing as a proportion of annual revenue

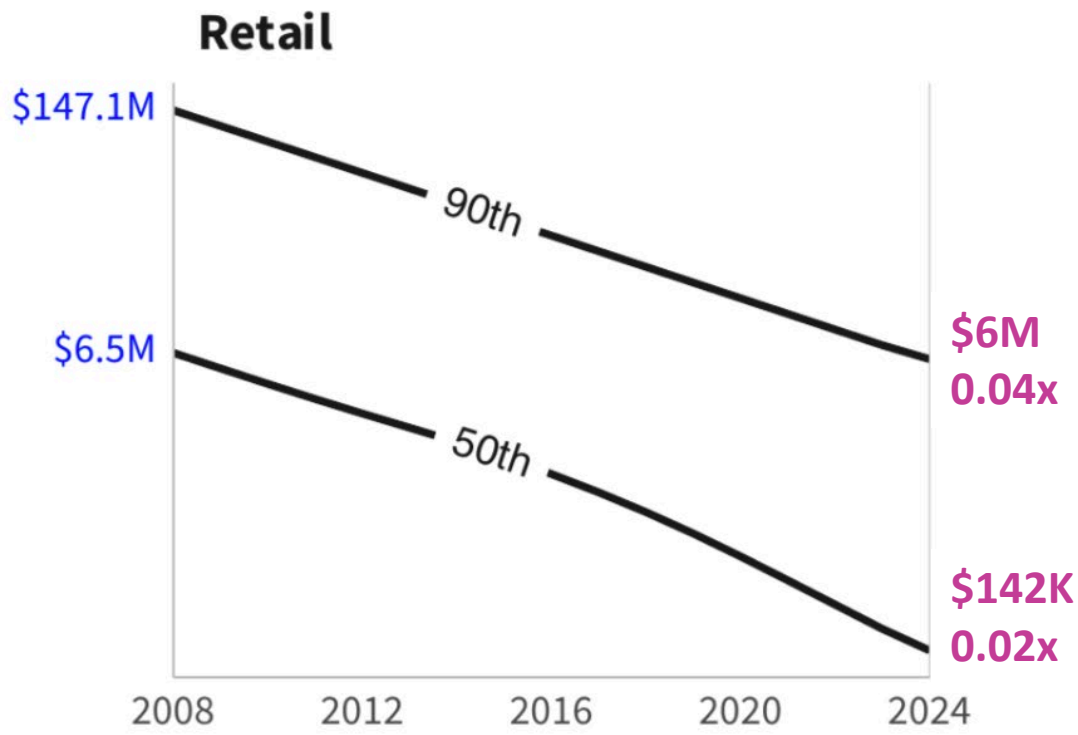
Revenue	Loss percentile 50%	95%
More than $10B	$2.2M	$130.3M
$1B to $10B	$2.1M	$44.0M
$100M to $1B	$581.0K	$11.8M
Less than $100M	$457.0K	$8.9M

Median and 95th percentile event losses by revenue tier



Losses up for some sectors; down for others





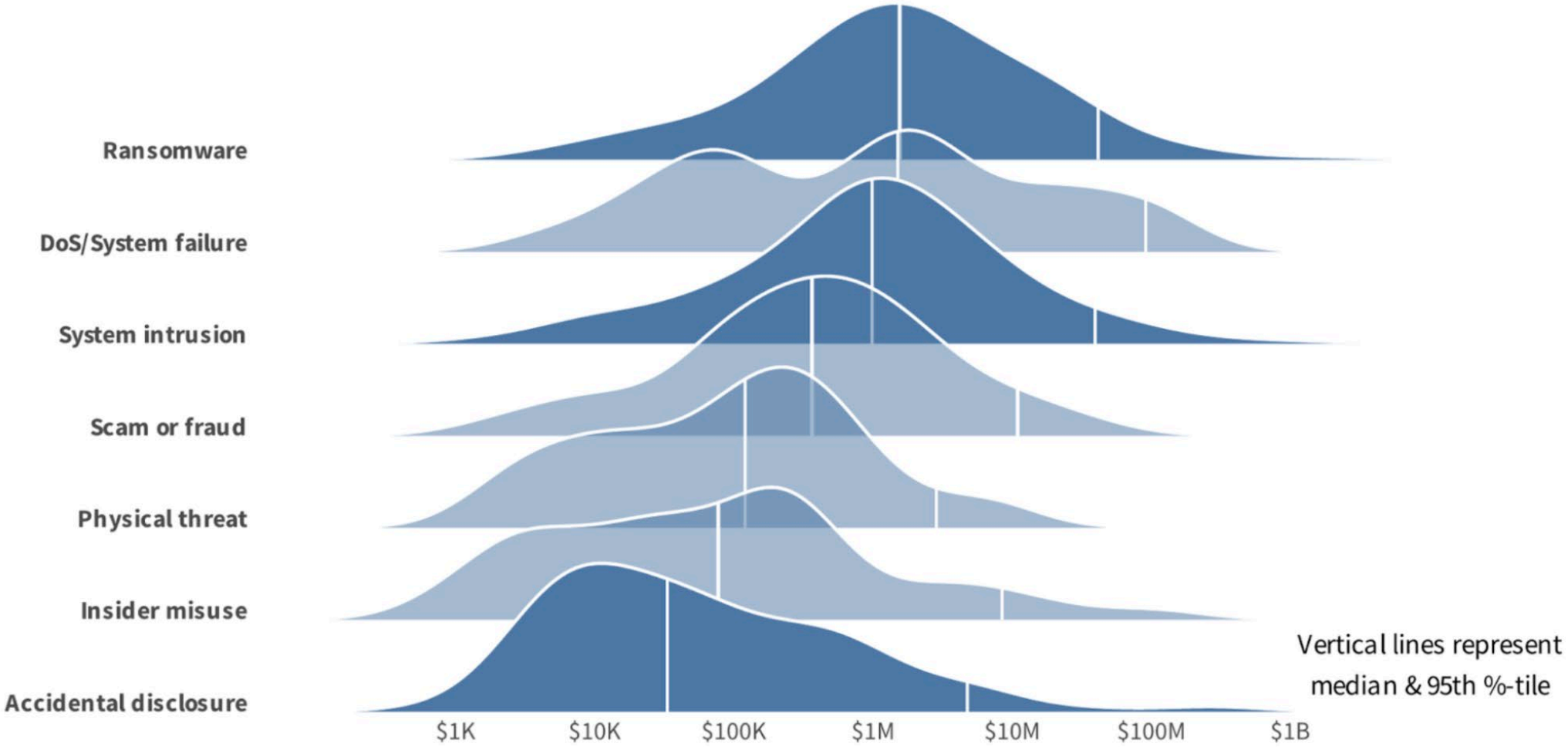
Trend analysis of median and 90th percentile event losses for example sectors

RSAC™ 2025 Conference

Do loss trends differ among event types?

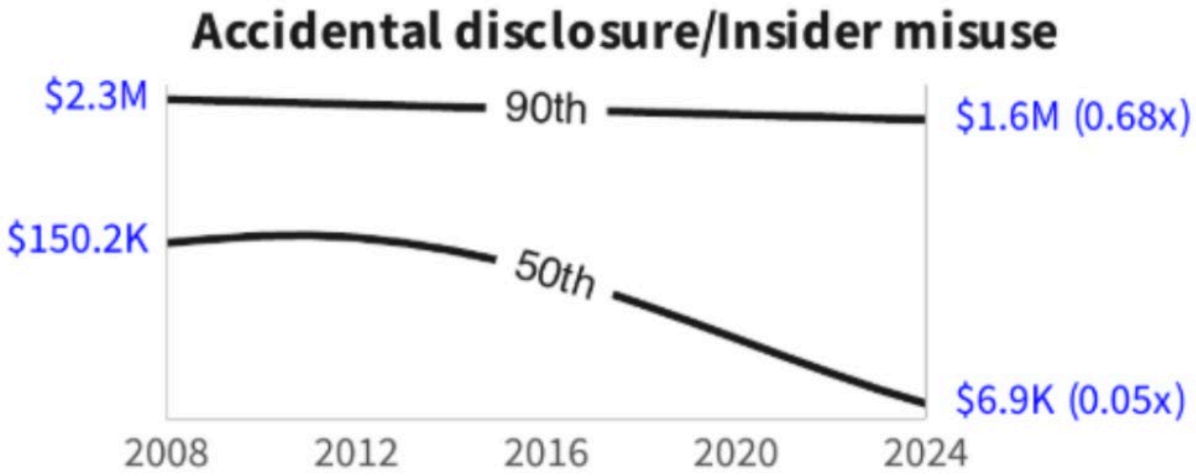
Many Voices.
One Community.

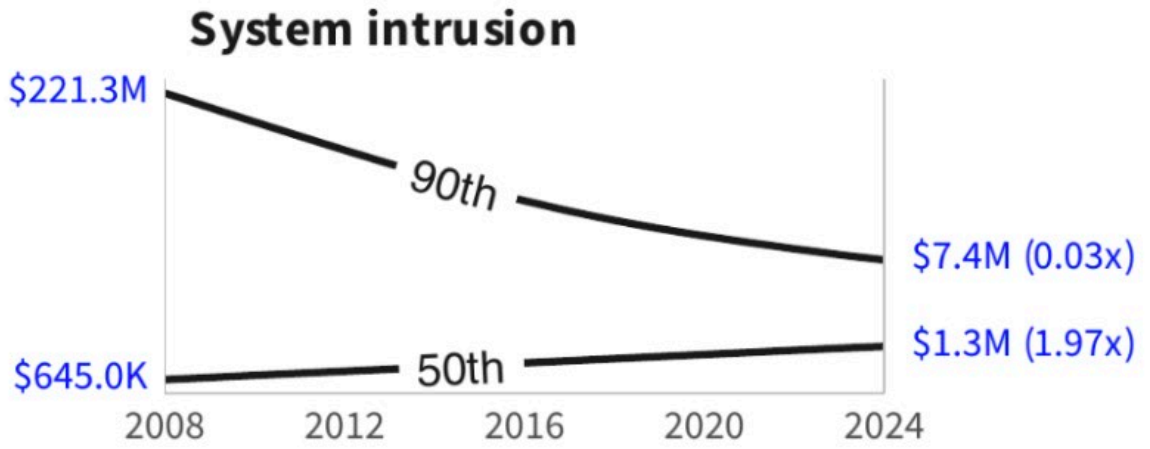
Loss distributions vary by incident type



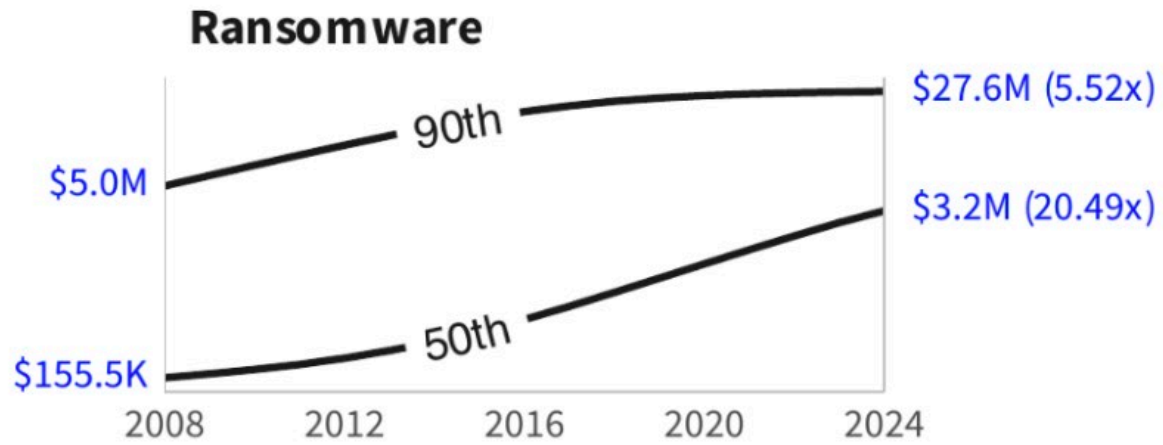
Distribution of reported losses by incident pattern (2008 to 2024)

Loss trends vary by incident type





Trend analysis of median and 90th percentile event losses by incident pattern

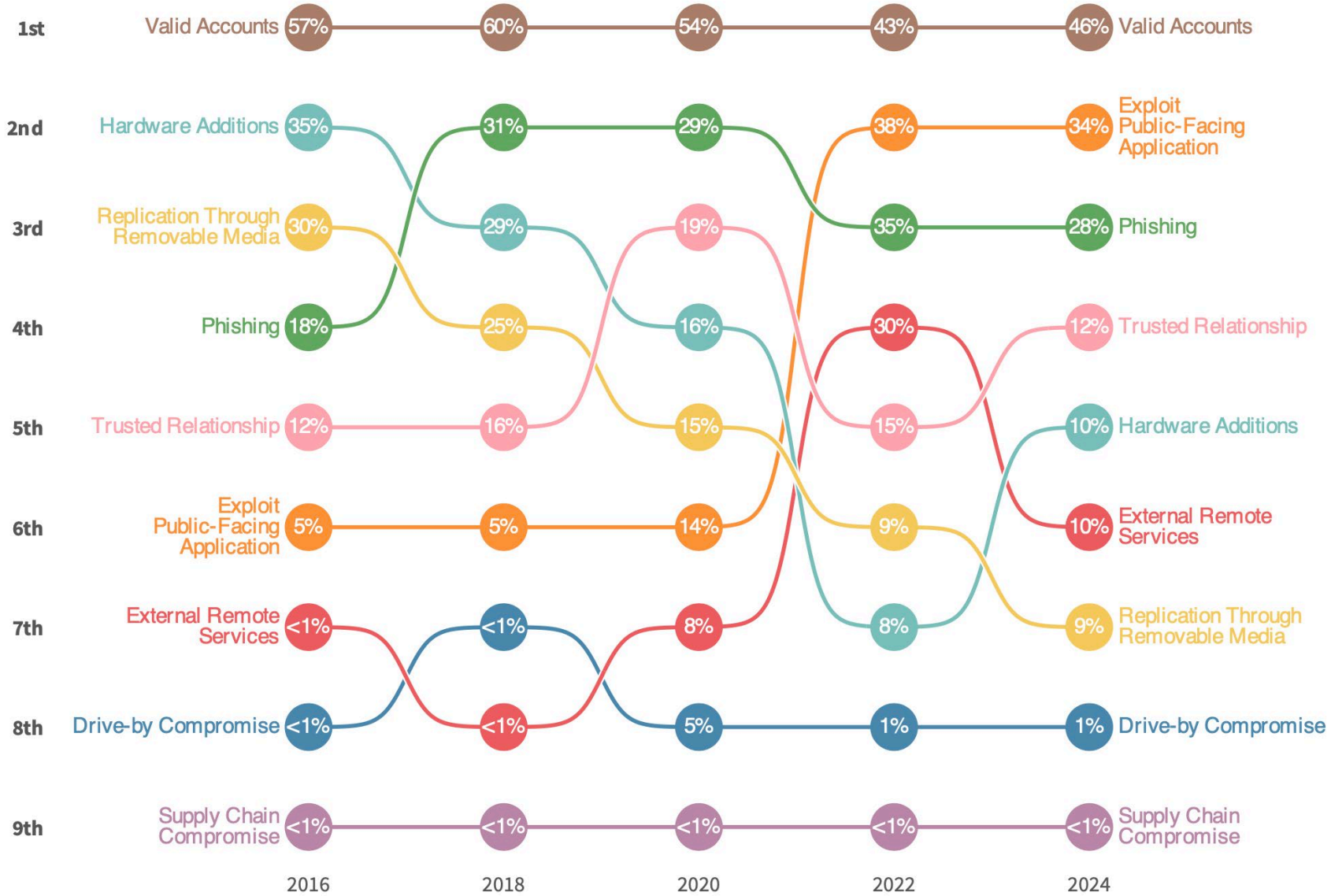


RSAC™ 2025 Conference

Are intrusion methods changing over time?

Many Voices.
One Community.

ATT&CK Initial Access techniques over time


1st
2nd
3rd
4th
5th
6th
7th
8th
9th
Valid Accounts 57% 60% 54% 43% 46% Valid Accounts
Hardware Additions 35% 31% 29% 38% 34% Exploit Public-Facing Application
Replication Through Removable Media 30% 29% 19% 35% 28% Phishing
Phishing 18% 25% 16% 30% 12% Trusted Relationship
Trusted Relationship 12% 16% 15% 15% 10% Hardware Additions
Exploit Public-Facing Application 5% 5% 14% 9% 10% External Remote Services
External Remote Services <1% <1% 8% 8% 9% Replication Through Removable Media
Drive-by Compromise <1% <1% 5% 1% 1% Drive-by Compromise
Supply Chain Compromise <1% <1% <1% <1% <1% Supply Chain Compromise
2016
2018
2020
2022
2024

Prevalence of ATT&CK Initial Access techniques observed in incidents over time

Supply chain compromise: Last place or Top 3?

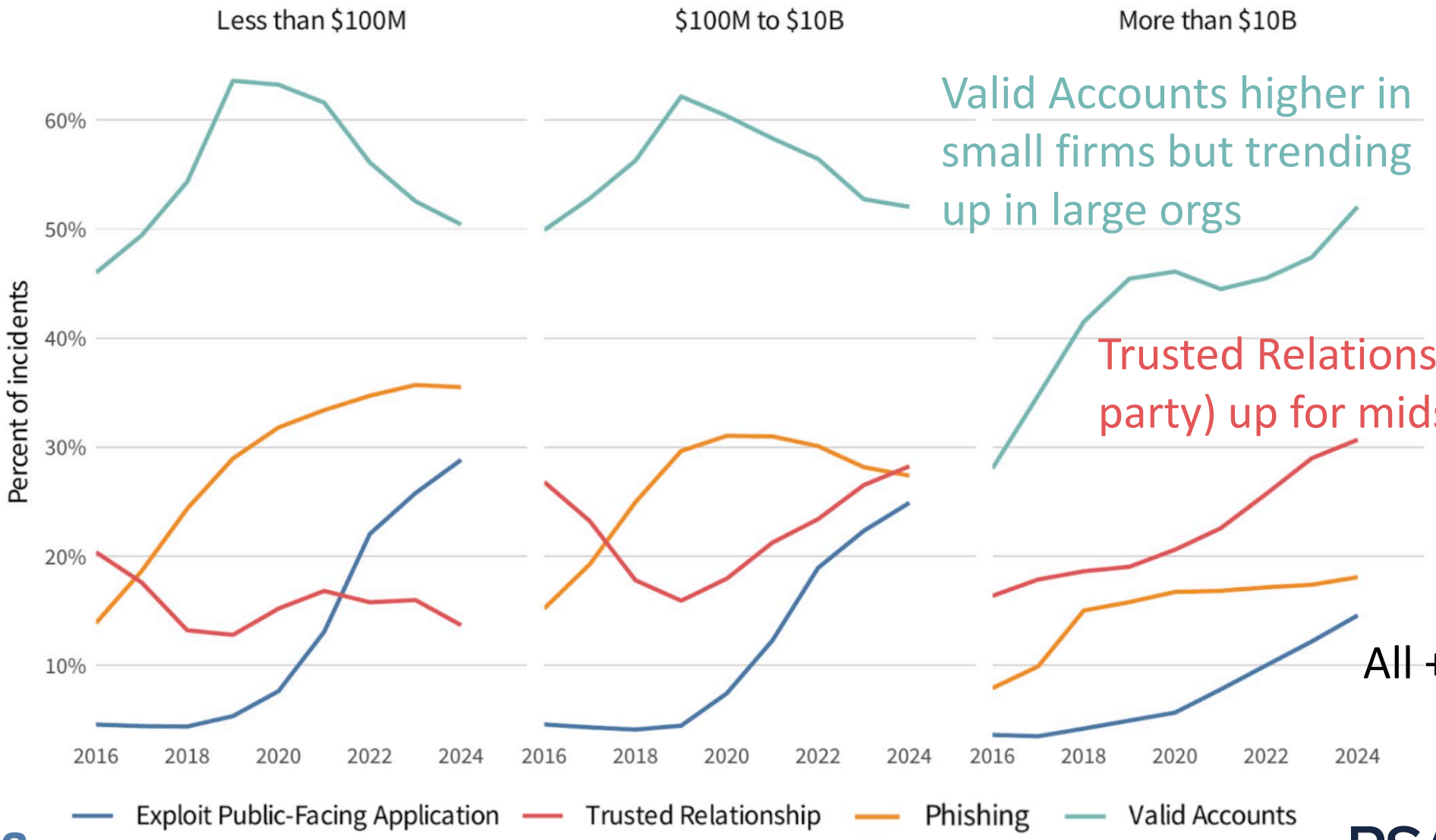
Frequency of MITRE ATT&CK Initital Access Techniques

Top ATT&CK initial access techniques identified by Cyentia (2014-2023 & 2024) and Feedly (2024)

Name	Cyentia (2014-2023)	Cyentia (2024)	Feedly
Phishing (T1566)	2nd	3rd	1st
Valid Accounts (T1078)	1st	1st	2nd
Exploit Public-Facing Application (T1190)	6th	2nd	6th
Supply Chain Compromise (T1195)	9th	9th	**3rd**
Hardware Additions (T1200)	**3rd**	**5th**	-
Drive-by Compromise (T1189)	8th	8th	4th
Replication Through Removable Media (T1091)	4th	7th	7th
Trusted Relationship (T1199)	**5th**	**4th**	-
External Remote Services (T1133)	7th	6th	5th

Comparison of top ATT&CK Initial Access techniques observed in incidents by source

Intrusion method trends vary by firm size



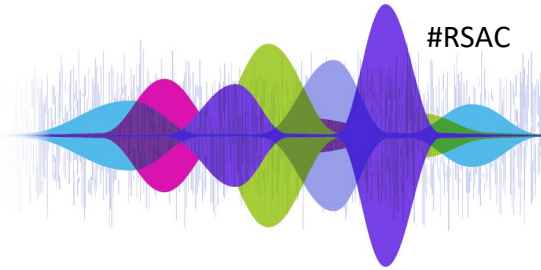
Valid Accounts higher in small firms but trending up in large orgs

Trusted Relationship (3rd party) up for midsize & large

All + for big biz

Prevalence of ATT&CK Initial Access techniques observed by revenue size

Apply What You Have Learned Today



- Next week you should:
  - Download & share the 2025 Information Risk Insights Study
  - www.cyentia.com/iris
- In 3 to 6 months following this presentation you should:
  - Begin monitoring key probability and loss trends among peer organizations
  - Assess your organization's risk exposure relative to its peers
- Over the next year you should:
  - Develop strategy & capabilities for risk-informed defense
  - Improve communication of key cyber risk trends to execs and board

RSAC™ 2025 Conference

Many Voices.
One Community.

CISA OCE: https://www.cisa.gov/about/divisions-offices/mission-enabling-offices/office-chief-economist

Cyentia IRIS 2025: https://www.cyentia.com/iris/